Survey on Searching Over Encrypted Data in Cloud

Smita Barkade[1], **Dr.S.A.Ubale**[2]
[1, 2] Department of Computer Engineering
[1, 2] Zeal College of Engineering & Research,Pune, India..

Abstract*-now a day's cloud computing is one of the most popular technique which allows user to share as well as store data on server and provide various on demand services. In cloud computing cloud users as well as provider of cloud service are mostly confidants to be from numerous trust domains. The services provided by cloud such as storing of data, sharing resources with multiple users can cause various security issues as well as access privilege issue due to untrusted access. Therefore trust, privacy as well as access control are the main problems while working with the cloud computing. Since access control allows the user to use resources in cloud. Cloud system allows multiple data owner and multiple data users to store and retrieve the outsourced data at a time. This survey provides a study of various methods designed by different researchers for searching on encrypted data on cloud.*

Keywords- Cloud computing, user revocation, ranking, attribute based encryption, data outsourcing.

I. INTRODUCTION

The rise in information and communication technologies (ICT) has modified the way people use their everyday data to work process and operations in business. As of late cloud computing has increased enormous consideration among analysts from both researchers and industry. It has developed as one of the promising advancements that is moving the processing worldview from conventional computing into the new time of cloud computing. The unavoidable access to dynamic unrestricted computing resources, system and communication framework with expanded versatility and adaptability has given figuring and correspondence to clients pervasively and at a moderate cost. Thus numerous establishments, associations and clients are relocating from customary processing situations to a cloud computing environment.

Cloud computing, as a rising paradigm, is sprouting in both research community and industry. It is characterized by the U.S. National Institute of Standards and Technology (NIST) as a model for empowering advantageous, on-request network access to a common pool of computing resources that can be quickly provisioned as well as discharged with minimum management efforts. Cloud computing empowers different cloud services to give framework, platform as well as programming for omnipresent correspondences and information get to. For instance, some mainstream cloud services, for example, Google Drive, iCloud and Dropbox, have liberated us from equipment limitations and guaranteed that the information we need is accessible whenever and wherever. Nonetheless, while grasping the services as well as advantages brought by cloud computing, we are likewise confronting the issues of information disclosure, privacy leaks and vindictive assaults.

At the time when cloud computing offer various advantages such as dynamic adaptability, whenever anyplace processing of data as well as communication, reduced cost of infrastructure, and so on, it additionally presents some new and repeating challenges in information computation & trustworthiness of communication, security and protection and so on. These difficulties have turned into a major worry in embracing cloud computing for health care, as information security and protection laws.

To ensure the security of sensitive data and battle unapproved gets to, delicate information ought to be encoded by the information owner before outsourcing. Be that as it may, encrypted information make the conventional information use benefit in light of plaintext keyword search pointless. The basic and ungainly strategy for downloading every one of the information and decrypting locally is clearly unfeasible, on the grounds that the information owner and other approved cloud clients must want to seek their interested information instead of the considerable number of information. Besides, the possibly tremendous number of outsourced information and great deal of cloud clients into thought, it is likewise hard to meet both the necessities of performance and system usability. Consequently, it is a particularly vital thing to investigate effective search service over encrypted outsourced data.

This survey presents the study of various systems generated by various researchers for searching over encrypted data and providing access control mechanism in cloud environment.

II.RELATED WORK

Searching over encrypted data can be accomplished by various secure search schemes which are actually based on either secret key cryptography (SKC) or public key cryptography (PKC). Curtmola et al. [1] presented an efficient single keyword encrypted data search scheme with the use of inverted index structure.

In this paper[2], for the first time ning cao,cong wang define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). Among various multi-keyword semantics, they choose the efficient similarity measure of “coordinate matching,” i.e., as many matches as possible, to capture the relevance of documents to the search query.

User authorization should be in place to grant multiple users search access.Hwang and Lee[3] in the public-key setting presented a conjunctive keyword search scheme in multi-user multi-owner scenario.But this scheme is not scalable under dynamic cloud environment.

To present practically-efficient secure search functions over encrypted data Wenhai Sun, and Bing Wang present a verifiable privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking To support
multi-keyword search and search result ranking, [4]propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy.

V. Goyal et al. [5] first introduced the concept of CP-ABE based on ABE. The main aim of this research is to develop secure type of attribute-based encryption cryptosystem. In this system each ciphertext is labeled by the encryptor with a set of expressive attributes. Each private key is connected with an access construction that specifies which type of ciphertexts the key can decrypt. They call such an idea a Key-Policy Attribute-Based Encryption (KP-ABE), since the access structure is specified in the private key, while the ciphertexts are simply labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if the attributes associated with a ciphertext satisfy the key's access structure. Their construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE)[5].

Wenhai Sun and Shucheng Yu [6] focused on different yet more challenging scenario multi-user and multi-contibutor i.e. data can be used from multiple data owners and searched by multiple users .And present first attribute-based keyword search scheme with efficient user revocation(ABKS-UR) which enables scalable fine-grained (i.e., file-level) search authorization. Developed system lets multiple owners to encrypt as well as outsource their information to the cloud server individually. Users can create their own search abilities not depending on an always online trusted authority. Also fine-grained search authorization is developed by the owner-enforced access policy on the index of every file.

In order to keep sensitive user data confidential from untrusted servers, it introduces a heavy computation overhead on the data owner for key distribution and data management. In paper [7] addressed this challenging open issue by defining and enforcing access policies based on data attributes and allowing the data owner to delegate most of the computation tasks to untrusted cloud servers without disclosing the underlying data contents.

Ming Li and Shucheng Yu et al.[8] propose a patient-centric framework and a set of mechanisms for data access control to PHRs stored in semitrusted servers. And also gives way for dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios

Table 1: Survey Table

Sr. No.	Title	Paper Details	Method Used	Advantages	Limitations
1.	Searchable symmetric encryption: Improved definitions and efficient constructions	Searchable symmetric encryption allows party to outsource the storage of data to another party in a private manner while maintaining the ability to selectively search over it.	extends inverted index approach in several non-trivial ways and introduces new techniques for the design of SSE	provide security for both indexes and trapdoors	secure against an adaptive adversary, but at the price of requiring a higher communication overhead per query and more storage at server
2.	Privacy-preserving multi-keyword	First time proposed privacy preserving multi	Co-ordinate matching i.e as	strict privacy requirements for	Used symmetric key cryptography which is

	ranked search over encrypted cloud data	keyword ranked search over encrypted data	many matches as possible and inner product similarity	such a secure cloud data utilization system	less flexible and allow less expressive search queries
3.	Public key encryption with conjunctive keyword search and its extension to a multi-user system	Presented a conjunctive keyword search scheme in multi-user multi-owner senario	construct an efficient PECK scheme whose security is proven over a decisional linear Diffie-Hellman assumption in the random oracle model	Public key settings used	Size of encrypted index and Search complexity proportional to no of users
4.	Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking	To support Multi - keyword search and search result ranking,	proposed search index based on term frequency and the vector space model with cosine similarity	Used Tree based index structure and adaptive methods for multidimensional algorithm to improve search efficiency	Support single user search setting no support for multi user
5.	Attribute-based encryption for fine-grained access control of encrypted data,	A new cryptosystem for fine-grained sharing of encrypted data -Key-Policy Attribute-Based Encryption (KPABE)	cipher texts are labeled with sets of attributes and private keys for access Structures	applicability for sharing of audit-log information and broadcast encryption	Do not hide the set of attributes under which the data is encrypted
6.	Protecting Your Right: Verifiable Attribute-Based Keyword Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud	Developed an attribute-based keyword search system having efficient user revocation	proxy re-encryption and lazy re-encryption techniques	Proposed scheme selectively secure against chosen-keyword attack.	scope for making user search more efficient
7.	Achieving secure, scalable, and fine-grained data access control in cloud computing	Enforced access policies based on data attributes and allows data owner to delegate most of the computation tasks to untrusted cloud servers.	combine techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.	It is highly efficient and provably secure underexisting security models.	Used KP-ABE but CP-ABE is more advanced
8.	Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption	Propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers.	divide the users in the PHR system into multiple security domains and on-demand user /attribute revocation and break-glass access under emergency scenarios	It supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios	For personal domain key management is with owner and thus key management scalability is overhead for large PHR

III. PROPOSED SYSTEM

To overcome the issues present in the existing system , we propose a system that is divided in three important entities such as, data owner, data server and data user. This system allows multiple data owner and multiple data users to store and retrieve the outsourced data at a time. This Proposed system is again characterized by two new features named as, User Revocation and Ranking of results. User Revocation enhances the security of data by protecting from unauthorized users and Ranking improves the satisfaction of user search experience.

IV. CONCLUSION

This survey provides the details of study of the various systems designed by different researchers for searching the encrypted data on cloud environment also listed their advantages and research gaps. To overcome the research gaps in the present system authors proposed a new system for searching the encrypted data in cloud environment..

REFERENCES

[1] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” in Proc. IEEE Conf. Comput. Commun., 2011, pp. 829–837.

[3] Y. H. Hwang, and P. J. Lee, “Public key encryption with conjunctive keyword search and its extension to a multi-user system,” in Proc. 1st Int. Conf. Pairing, 2007, pp. 2–22.

[4] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, “Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 11, pp. 3025–3035, Nov. 2014.

[5] Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[6] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: Attribute-based keyword search with fine-grained owner enforced search authorization in the cloud,” in Proc. IEEE Trans on Parallel Distrib. Syst., vol. 27, no. 4, Apr. 2016.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable,and fine-grained data access control in cloud computing,” in Proc. IEEE Conf. Comput. Commun., 2010, pp. 1–9.

[8] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Trans. Parallel Distrib. Syst,vol. 24, no. 1, pp. 131–143, Jan. 2013.